UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OKLAHOMA

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) TO DISCLOSE CERTAIN RECORDS PERTAINING TO A GOOGLE, INC. EMAIL ACCOUNT	MISC. NO. 19-MJ-119-JFJ **Filed Under Seal**

APPLICATION FOR 18 U.S.C. § 2703(d), SEALING, AND NONDISCLOSURE ORDER

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc. ("Google"), an electronic communications services provider and/or remote computing service located in Mountain View, California, to disclose certain records and other information pertaining to the e-mail account, as described in Part I of Attachment A. The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c).

2. This Court has jurisdiction to issue the proposed Order because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i). *See* 18 U.S.C. § 2711(3)(A)(ii).

3. A court order under § 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

4. The Federal Bureau of Investigation (FBI) is investigating violations of federal law including, but not limited to, Title 18 Section 1343 (Wire Fraud) stemming from the victimization of Tulsa, Oklahoma-based company XRG Technologies (hereinafter referred to as "XRG").

5. By way of background, business e-mail compromise is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfers. The scam is commonly carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Additionally, the scams can also rely on social engineering and deception to convince victims to send money, usually via a wire transfer, to criminal actors. The scam is commonly initiated when a victim receives false wire instructions from a criminal who is masquerading as a trusted business contact.

6. The FBI was first contacted by an XRG Vice President (hereinafter referred to as "BH") on or about May 6, 2019. BH told the FBI that unknown individual(s) obtained unauthorized access to her e-mail account and modified payment wiring instructions on invoices.

7. BH also provided the FBI with copies of some e-mails sent and received from her XRG e-mail account. A review of the e-mails revealed BH received an e-mail from e-mail address o.wuttke@schrnidt-clemens.com on or about April 1, 2019 with a "revised invoice" attached. BH later identified Oliver Wuttke as an employee of Schmidt-Clemens and confirmed the company was one of XRG's vendors; however, BH and the FBI noted the originating e-mail address above substituted the letters "r" and "n" for "m." The FBI believes the criminal actor was attempting to masquerade as XRG's legitimate vendor by using an altered e-mail address.

8. After receiving the e-mail from o.wuttke@schrnidt-clemens.com on or about April 1, 2019 with the "revised invoice," BH authorized a wire transfer of approximately $686,000. BH became aware there was a problem on or about May 6, 2019, after being contacted by Schmidt-Clemens regarding the status of the payment. BH then closely reviewed her e-mails and noted the difference in the e-mail addresses.

9. The FBI discovered that the bank wire BH had authorized was actually sent to a bank account in Asia. The FBI is currently pursuing a Mutual Legal Assistance Treaty (MLAT) request to gather further information regarding the bank account.

10. On May 31, 2019, the FBI performed research on the domain "schrnidt-clemens.com" and identified the domain's MX (mail exchange) server as aspmx.l.google.com. Consequently, the FBI believes electronic communications records for e-mail address o.wuttke@schrnidt-clemens.com are stored at a premises maintained by Google.

REQUEST FOR ORDER

11. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the United States requests that Google be directed to produce all items described in Part II of Attachment A to the proposed Order.

12. The United States further requests that the Order require Google not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order for a time period of one year. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the attached court order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Additionally, extensive coordination with foreign law enforcement entities will be required to acquire and execute an MLAT request. MLAT requests typically average around nine months from request to completion and can often take over a year. Accordingly, there is reason to believe that notification of the existence of the attached court order will seriously jeopardize the investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, or notify confederates.

13. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation and is expected to take at least a year to complete. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

R. TRENT SHORES
UNITED STATES ATTORNEY

By: _____
Christopher J. Nassar
Assistant United States Attorney

ATTACHMENT A

I. Target Account

This order applies to certain records and information of the Provider associated with any accounts associated with the following e-mail address (the "Target Account"):

o.wuttke@schrnidt-clemens.com

II. Records and Other Information to Be Disclosed

Google is required to disclose the following records and other information, if available, to the United States for the account listed in Part I of this Attachment (the "Target Account"), for the time period from the inception of the account to the present:

A. All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login Internet Protocol ("IP") address, recovery e-mail or phone number, Android ID, Google ID, or otherwise) ("Linked Accounts"); and, for each Linked Account, all records and information described in subsections II.B through II.E of this Attachment.

B. All accounts that are registered or subscribed using the Target Account or any Linked Accounts (i.e. with any one of the Target Account or any Linked Accounts in any subscriber information).

C. Any and all cookies associated with or used by any computer or web browser associated with the Target Account or any Linked Accounts, including the IP addresses, dates, and times associated with the recognition of any such cookie.

D. The following information about the customers or subscribers of the Target Account or any Linked Accounts:

1. Names (including subscriber names, user names, and screennames);

2. Addresses (including mailing addresses, residential addresses, business addresses, and additional and rescue e-mail addresses);
3. Local and long distance telephone connection records;
4. Length of service (including start date) and types of service utilized;
5. Other subscriber numbers or identities (including the registration IP address); and
6. Means and source of payment for such service (including any credit card or bank account number) and billing records.

E. All records and other information (not including the contents of communications) relating to the Target Account or any Linked Accounts, including:

1. Records of user activity for each connection made to or from the account, including records of session times and durations and the temporarily assigned network addresses (such as IP addresses) and telephone or instrument numbers (including MAC addresses) associated with those sessions; log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination IP addresses;
2. Information about each communication sent or received by the account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers); and
3. Accounts to which any Linked Accounts are themselves linked, other than by the Target Account, including by cookie, creation or login IP, e-mail, recovery email, phone number, or otherwise.